ANALISA SERANGAN *REMOTE EXPLOIT* MELALUI *JAVA APPLET ATTACK METHOD* TERHADAP SISTEM OPERASI *WINDOWS* 8

SKRIPSI

Disusun Sebagai Salah Satu Syarat Menyelesaikan Jenjang Strata I
Program Studi Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Oleh:

Bryan Pingkan Ramadhan
NIM : L200110143

PROGRAM STUDI INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
JULI 2015

HALAMAN PERSETUJUAN

Skripsi dengan judul

ANALISA SERANGAN *REMOTE EXPLOIT* MELALUI *JAVA APPLET*

***ATTACK METHOD* TERHADAP SISTEM OPERASI *WINDOWS* 8**

Telah diperiksa, disetujui dan disahkan pada :

Hari : Sabtu

Tanggal : 11 Juli 2015

Pembimbing

Gunawan Ariyanto, Ph.D.

NIK : 968

HALAMAN PENGESAHAN

ANALISA SERANGAN *REMOTE EXPLOIT* MELALUI *JAVA APPLET ATTACK METHOD* TERHADAP SISTEM OPERASI *WINDOWS* 8

Dipersiapkan dan disusun oleh

Bryan Pingkan Ramadan

NIM : L200110143

Telah dipertahankan di depan Dewan Penguji

Pada tanggal 4 Juli 2015

Susunan Dewan Penguji

Pembimbing

Gunawan Ariyanto, PhD.
NIK : 968

Dewan Penguji I	Dewan Penguji II
Muhammad Kusban, S.T., M.T.	Dr. Heru Supriyono, M.Sc.
NIK : 663	NIK : 970

Skripsi ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal 3 Agustus 2015

Dekan Fakultas Komunikasi dan Informatika	Ketua Program Studi Informatika
Husni Thamrin, S.T.,MT.,Ph.D.	Dr. Heru Supriyono, M.Sc.
NIK :706	NIK : 970

KONTRIBUSI

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut ini saya sampaikan daftar kontribusi dalam penyusunan skripsi :

1. Penelitian dilakukan dengan menggunakan aplikasi *Metasploit framework, Wireshark, Volatility, CapureBat, FTK Imager, Comodo Firewall* dan *JD-GUI* yang merupakan aplikasi *freeware.*
2. Penulis menganalisa serangan tersebut dengan beberapa referensi baik journal, skripsi, buku maupun internet.
3. Persiapan dari mulai peralatan penelitian dan tahap konfigurasi dilakukan oleh penulis sendiri.
4. Penulisan skripsi laporan ini murni dilakukan oleh penulis.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggung jawab atas ini dan kebenaran diatas.

Surakarta, Mei 2015

Mengetahui Pembimbing Tugas Akhir	Penulis
Gunawan Ariyanto, Ph.D.	**Bryan Pingkan Ramadhan**
NIK : 968	

MOTTO

"Maka sesungguhnya bersama kesulitan itu ada kemudahan.

Sesungguhnya bersama kesulitan itu ada kemudahan."

(Q.S. Al-Insyirah : 5-6)

"Perang yang perlu dilakukan sekarang adalah perang terhadap ketidaktahuanmu bahwa dirimu masih dalam penjara. Dan penjaranya adalah ukuran-ukuran dalam fikiranmu yang bukan berasal dari dirimu sendiri ."

(Sabrang MDP)

" Kalau kita tidak memiliki kedaulatan atas diri kita, kalau kita tidak berdaulat atas apa yang kita putuskan sebagai belief system dalam diri kita maka orisinalitas tidak akan kita temukan."

(Sabrang MDP)

"Kebenaran yang sesungguhnya tidak akan pernah bisa dicapai, yang bisa dilakukan hanyalah terus mencari."

(Penulis)

PERSEMBAHAN

Sebagai rasa syukur dan terima kasih saya persembahkan skripsi ini kepada:

1. Allah SWT yang selalu memberikan kesehatan, kelapangan ilmu dan kemudahan jalan dalam mengerjakan skripsi ini.
2. Orang tuaku tercinta Bapak Mujiyono dan Ibu Surani yang selalu memberikan semangat, motivasi, dan senantiasa mendoakan untuk kebahagiaan dan kesuksesanku dengan penuh keikhlasan.
3. Adikku Prasetya Tegar Fitriaji yang selalu memberikan pengertian dan doa untuk penulis.
4. Bapak Gunawan Ariyanto, Ph.D. yang telah membimbing saya, terima kasih atas semuanya dan maafkan jika ada tutur kata ataupun ada tingkah laku yang kurang baik selama ini.
5. Teman-teman IDM karpet biru angkatan 2011 terima kasih atas keceriaan dan semangat yang diberikan.
6. Mas Aji Saputra sebagai biro skripsi yang telah banyak membantu.
7. Keluarga besar Program Studi Informatika Universitas Muhammadiyah Surakarta.

KATA PENGANTAR

Alhamdulillah, puji syukur kami panjatkan kepada Allah SWT yang telah melimpahkan rahmat dan hidayahNya sehingga penulis dapat menyelesaikan skripsi dengan judul "Analisa Serangan *Remote Exploi*t Melalui *Java Applet Attack Method* Terhadap Sistem Operasi *Windows* 8".

Skripsi ini disusun untuk memenuhi kurikulum pada Program Studi Informatika Universitas Muhammadiyah Surakarta, sebagai kewajiban mahasiswa dalam rangka menyelesaikan program sarjana.

Dengan segala kemampuan yang dimiliki, penulis telah berusaha untuk menyelesaikan laporan skripsi ini. Namun penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan dan masih banyak kekurangan. Oleh sebab itu penulis berkenan menerima saran dan kritik yang bersifat membangun demi perbaikan laporan ini. Di sisi lain, skripsi ini juga merupakan hasil karya dan kerja sama semua pihak, walaupun yang terlihat hanya sebuah nama. Sehingga dalam kesempatan ini, penulis mengucapkan terima kasih dan penghargaan setinggi-tingginya dengan segala kerendahan hati, kepada :

1. Bapak Husni Thamrin, S.T, MT., Ph.D. selaku Dekan Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.
2. Bapak Dr. Heru Supriyono, M.Sc. selaku Ketua Program Studi Informatika Universitas Muhammadiyah Surakarta.
3. Bapak Fatah Yasin Irsyadi, S.T., M.T. selaku Pembimbing Akademik.
4. Bapak Gunawan Ariyanto, Ph.D. selaku pembimbing skripsi yang telah memberikan bimbingan dan pengarahan dalam penyusunan skripsi ini.

5. Segenap dosen Universitas Muhammadiyah Surakarta yang telah memberikan ilmu kepada penulis.
6. Kedua orang tua yang selalu mendoakan dan memberikan semangat dalam penyusunan skripsi ini.
7. Teman-teman IDM karpet biru yang telah bersama selama 4 tahun ini, terima kasih atas keceriaan yang telah dibagikan.
8. Semua pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu.

Surakarta, Mei 2015

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAKSI

Dalam 5 tahun terakhir jenis serangan *client-side attacks* jumlahnya meningkat secara dramatis. penyerang mengalihkan fokus mereka ke sisi klien yang memiliki celah lebih besar karena klien mempunyai perlindungan terhadap sistem yang lebih sederhana daripada *server.* Eksploitasi dengan menggunakan *malicous Java* yang memanfaatkan kerentanan pada *Java* adalah yang paling sering terdeteksi oleh *Trustwave Secure Web Gateway anti-malware technology* dengan persentase sebesar 78% dan sebagian besar penjahat *cyber* mengandalkan *Java applet* sebagai metode untuk mengirimkan *malware* maupun *payload*. *Java applet attack method* adalah salah satu teknik serangan yang memanfaatkan kerentananan pada *Java* untuk mengeksploitasi sistem *user* menggunakan *Java applet* dan dapat menyerang ke berbagai sistem operasi termasuk *Windows* 8 yang merupakan sistem operasi keluaran terbaru dari *Microsoft*. Skripsi ini bertujuan untuk menganalisa serangan *remote exploit* melalui *Java applet attack method* terhadap sistem operasi *Windows* 8 yang terproteksi *firewall*.

Penelitian yang dilakukan menggunakan metode studi pustaka dan melakukan eksperimen yang melalui beberapa tahapan diantaranya studi kepustakaan, pengolahan data, pengujian serangan, analisa serangan, optimalisasi *firewall,* pengujian *firewall* dan penulisan laporan. Dengan menganalisa serangan tersebut akan diketahui perilaku dan karakterisiknya, karakteristik dari serangan tersebut terletak pada *Java exploit* dan *Java payload* yang ada didalam *Java applet*. *Java exploit* berfungsi untuk melewati *Java Virtual Machine* (JVM) *sandbox* dan menonaktifkan *SecurityManager* dan *payload Java meterpreter* berfungsi untuk mengelabuhi *firewall* dan sebagai media interaksi antara penyerang dengan sistem klien. Kemudian dibuat *rule firewall* pada *Comodo Firewall* yang mampu mencegah *payload* untuk melakukan *reverse connection* dan mencegah *payload* melakukan *staging*.

Kata Kunci : *Remote exploit***,** *Java applet attack method, Windows 8, firewall.*